WHATLEY KALLAS, LLP
Alan M. Mansfield, SBN: 125998
16870 W. Bernardo Drive
Suite 400
San Diego, CA 92127
Phone: (619) 308-5034
Fax: (888) 341-5048
Email: amansfield@whatleykallas.com

Attorneys for Plaintiff

[Additional Counsel on Signature Page]

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

JOHN DOE, on behalf of himself and all others similarly situated and for the benefit of the general public,

Plaintiff,

v.

PARKER-HANNIFIN CORPORATION, and DOES 1 through 10, inclusive,

Defendants.

Case No.

CLASS ACTION COMPLAINT FOR VIOLATIONS OF:

(1) California Consumer Privacy Act
(2) Confidentiality of Medical Information Act
(3) Invasion of Privacy
(4) Unlawful and Unfair Business Practices
(5) Declaratory Relief

Jury Trial Demanded on All Causes of Action So Triable

Plaintiff John Doe ("Plaintiff"),[1] brings this action on behalf of himself and all others similarly situated and for the benefit of the general public against Defendant Parker-Hannifin Corp. ("PARKER-HANNIFIN" or "Defendant") and DOES 1–10, inclusive (collectively referred to herein as "Defendants"). Plaintiff, through his undersigned counsel, alleges the following based on personal knowledge as to allegations regarding Plaintiff, and on information and belief as to all other allegations, which allegations are likely to have evidentiary support after a reasonable opportunity for investigation and discovery.

SUMMARY OF THE ACTION

1. Plaintiff brings this class action lawsuit his own behalf, and on behalf of a class of similarly situated individuals defined below and for the benefit of the general public, against Defendants arising from the failure by PARKER-HANNIFIN to adequately secure the Personal Information and/or Medical Information (defined below) of Plaintiff and all others similarly situated who are current residents and citizens of California.

2. As detailed more fully below, in March 2022 PARKER-HANNIFIN was subject to a ransomware attack and accompanying data breach and theft by the Conti ransomware group ("Conti"). On or about March 11, 2022, Conti gained access to Defendant PARKER-HANNIFIN's computer network, deployed malware that encrypted data in PARKER-HANNIFIN's servers, and acquired over 400 gigabytes of employees' personal information stored on Defendant PARKER-HANNIFIN's computer network servers (the "Data Breach"). It appears PARKER-HANNIFIN did not make a ransomware payment, as now all of this employee data is available on the dark web. This impacted Plaintiff and other similarly situated individuals who either are or were employed by PARKER-HANNIFIN or are or were enrolled in PARKER-HANNIFIN's Group Health Plan or a health plan sponsored by an entity acquired by PARKER-HANNIFIN.

3. PARKER-HANNIFIN negligently created, maintained, preserved, and stored on its computer systems Plaintiff's and Class members' personally individually identifiable Personal

[1] Due to the sensitive nature of this action and the fact his information appears to be available on the dark web, Plaintiff has elected to file under a pseudonym. (*See, e.g., Doe v. Kaweah Delta Hosp.*, 2010 U.S. Dist. LEXIS 135808 (E.D. Cal., Dec. 22, 2010); *Does I thru XXIII v. Advanced Textile Corp*. 214 F.3d 1058, 1067 (9th Cir. 2000).

Information and/or Medical Information. The personal information that may have been accessed and taken includes PARKER-HANNIFIN and its subsidiaries employees' full names, Social Security numbers, dates of birth, addresses, driver's license numbers, U.S. passport numbers, bank account and routing numbers, online usernames and passwords ("Personal Information"). PARKER-HANNIFIN failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the information at issue in order to protect Plaintiff's and others' personal information, which would include Personal Information and Medical Information. Defendants' actions resulted in this information being improperly accessed and copied by unauthorized third parties.

4. Defendants either knew, or reasonably should have known, the importance of safeguarding the Medical Information and Personal Information entrusted to them and of the foreseeable consequences if their computer network was breached. Defendants failed, however, to take adequate measures to prevent the Conti ransomware attack. Defendants were on notice that they should have and could have prevented this attack by properly securing and encrypting the information of Plaintiff and the Class members and taking the steps outlined above to prevent infiltration by methods such as phishing by, for example, using multi-factor authentication methods. Defendants could also have destroyed data of former employees and their dependents that was no longer useful, especially outdated data for individuals who either never worked for PARKER-HANNIFIN or left their employ years ago that for some reason was retained on its computer network.

5. As a result, the Personal Information and Medical Information of a reported 119,513 individuals was compromised through disclosure to unknown and unauthorized third parties. PARKER-HANNIFIN thus disclosed and/or permitted the disclosure of these persons' Medical Information and Personal Information to unauthorized persons. An unknown but likely significant number of such persons are residents and citizens of California and thus entitled to the unique statutory remedies available under California law.

6. Defendants' employees negligently created, maintained, preserved, and stored Plaintiff's and Class members' personally individually identifiable "medical information," within the meaning of Civil Code section 56.05(i). Defendants' actions resulted in this medical information being improperly accessed and copied by unauthorized third parties.

7. Article 1, section 1 of the California Constitution guarantees consumers their right to privacy. In addition, as recognized by the California Legislature, the use of sophisticated computer information technology has greatly magnified the potential risk to individual privacy that occurs from the maintenance of personal information by entities such as Defendants, necessitating that the maintenance of personal information is subject to strict limits governed by numerous California statutes.[2]

8. Medical information in California is considered to be among the most sensitive private personal information available.[3] "Medical Information" is defined by California's Confidential Medical Information Act, Cal. Civ. Code sections 56, *et seq*. ("CMIA") as:

> any individually identifiable information, in electronic or physical form, in possession of or derived from a provider of health care, health care service plan, pharmaceutical company, or contractor regarding a patient's medical history, mental or physical condition, or treatment.
>
> "Individually identifiable" means that the Medical Information includes or contains any element of personal identifying information sufficient to allow identification of the individual, such as the patient's name, address, electronic mail address, telephone number, or Social Security Number, or other information that, alone or in combination with other publicly available information, reveals the identity of the individual.[4]

9. "Medical Information", for purposes of this Complaint, includes health plan enrollment information, health insurance plan ID numbers, and dates of coverage, and for a small subset of individuals, the following sensitive information that may also have been accessed and acquired: dates of medical coverage, dates of medical services, provider names, claims information and medical and clinical treatment information. This term also refers to the above definition, and encompasses both Personal Health Information ("PHI"), and Personally Identifiable Information ("PII"), including Social Security numbers associated with individual health records within PARKER-HANNIFIN's computer systems.

10. Since Medical Information encompasses such personal and revealing information, it is highly valued as a gateway to medical identity theft[5] and more general identity theft.[6] Medical Information has been found to command up to $1,000 per individual record on the dark web.[7] Thus,

---

[2] See Cal. Civil Code § 1798.1(b) & (c).
[3] *See, e.g.*, Cal. Civ. Code § 1798.140(ae)(2)(B) (as amended by Proposition 24) (defining health information as sensitive data).
[4] Cal. Civ. Code § 56.05(i).
[5] R. Kam, *et al, Medical Identity Theft: A Deadly Side Effect of Healthcare Data Breaches*, ID Experts (2017).
[6] Identity Theft Resource Center, *Data Breaches in the Healthcare Industry Continue Due to Availability of Valuable Information* (8/11/2020).
[7] M. Yao, *Your Electronic Medical Records Could be Worth $1,000 to Hackers*, Forbes (4/18/17).

organizations such as Defendants, who are entrusted with this most sensitive and valuable data, have a non-delegable duty to take particularly special care to maintain up-to-date information security practices and keep apprised of industry-related threats as they arise. The threat from the Conti group of a ransomware attack was reasonably foreseeable to Defendants, as companies had been warned for almost a year of the potential for such an attack on their computer systems.

11. Companies such as PARKER-HANNIFIN are legally required and have a duty to keep their employees' Personal Information and Medical Information private and secured. Defendants breached duties owed to Plaintiff and Class members by, *inter alia*, (i) not exercising reasonable care in retaining, maintaining, securing, and safeguarding current and former employees' nonpublic Personal Information and Medical Information from being accessed and stolen by unauthorized persons; (ii) failing to implement processes to detect a breach or unauthorized access in a timely manner and to promptly act upon any warnings or alerts that Defendants' security systems had been breached or improperly accessed; (iii) failing to timely disclose the facts surrounding this breach to Plaintiff and Class members; and (iv) failing to disclose that Defendants could not or did not adequately secure Plaintiff's or Class members' Personal Information and Medical Information.

12. Under the CMIA and other provisions of law referenced herein, Plaintiff and all other persons similarly situated have a recognized right to confidentiality in their personal Medical Information and can reasonably expect that their Medical Information would be protected by Defendants from unauthorized access. When Plaintiff and all other persons similarly situated provided their Medical Information to PARKER-HANNIFIN for the purpose of health plan enrollment, maintaining a health plan account with PARKER-HANNIFIN and/or otherwise availing themselves of health care services through PARKER-HANNIFIN, they did so with the reasonable understanding and assurance that their most sensitive medical and personal information would be kept confidential and secure.

13. The Historical and Statutory Notes for the short title of the CMIA, section 56, support these reasonable expectations:

> The Legislature hereby finds and declares that persons receiving health care services have a right to expect that the confidentiality of individual identifiable Medical Information derived by health service providers be reasonably preserved. It is the intention of the Legislature in enacting this act, to provide for the confidentiality of individually identifiable Medical Information, while permitting certain reasonable and limited uses of that information.

14. Consistent with that statutory purpose, the CMIA provides that "a provider of health care, health care service plan, or contractor shall not disclose Medical Information regarding a patient of the provider of health care or an enrollee or subscriber of a health care service plan without first obtaining an authorization [. . .]." (Cal. Civ. Code § 56.10(a).) Defendants' actions permitted the disclosure of the Medical Information at issue here to unauthorized third parties.

15. Additionally, Civ. Code Section 56.101(a) states, in relevant part, that every health care provider or health care service plan that creates, maintains, preserves, or stores Medical Information shall do so in a manner that preserves its confidentiality. Defendants' actions establish that they did not maintain the Medical Information at issue in a manner that preserved its confidentiality, as it was able to be improperly accessed and copied by unauthorized third parties, including the Conti group. PARKER-HANNIFIN's failure to create, maintain, preserve, and store Medical Information in a manner that preserved the confidentiality of the information contained therein resulted in the illegal access, authorization, exfiltration, disclosure, negligent release and/or theft of over 400 gigabytes of data related to PARKER-HANNIFIN current and former employees, their dependents and members of PARKER-HANNIFIN's group health plans (including health plans sponsored by an entity acquired by PARKER-HANNIFIN), which necessarily included PII, PHI and Medical Information.

16. Defendants had obligations under California Civil Code Sections 56.20(a) and (c) to ensure, as an employer, that (1) if they received Medical Information about their employees, that they would establish appropriate procedures to ensure the confidentiality and protection from unauthorized use and disclosure of that information; and (2) that they would not disclose or knowingly permit their employees or agents to disclose Medical Information about their employees without a signed authorization.

17. Defendants' violations of California Civil Code §§ 56.20(a) and (c) subject them to the remedies afforded under California Civil Code §§ 56.35 and 56.36(b).

18. The remedies provided for under California Civil Code Section 56.35 allow private litigants whose Medical Information has been used or disclosed in violation of California Civil Code § 56.20 or/and who have sustained economic loss to recover compensatory damages, punitive damages not to exceed $3,000 per class member, attorney fees not to exceed $1,000 per class member and the costs

of litigation. However, these are only partial remedies as they do not resolve the underlying issue, protecting Plaintiff and Class members from misuse of their data or further attacks, including, but not limited to, fraudulent use of their financial information, identity theft, use of their medical information to fraudulently secure and pay for medical services, use of Social Security numbers to file false tax returns, steal tax refunds or gain employment under an assumed identity, and opening credit under false credentials. Nor do these monetary remedies help Plaintiff and Class members monitor or remove this data to prevent further abuses on the dark web.

19. Defendants disregarded the rights of Plaintiff and members of the Class by negligently failing to take and implement adequate and reasonable measures to ensure that Plaintiff's and the Class members' Personal Information and Medical Information was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required and appropriate protocols, policies and procedures regarding data access and encryption, even for internal use, as well as appropriate procedures that would prevent such intrusions through methods such as phishing, like multi-factor authentication..

20. Defendants' actions additionally violated the California Consumer Privacy Act ("CCPA"), California Code §§ 1798.100 *et seq.,* in that they failed to keep the nonencrypted and nonredacted personal information of Plaintiff and all similarly situated persons from unauthorized access and exfiltration, theft or disclosure as a result of Defendants' violation of their duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect that Personal Information. The personal information at issue relevant to this violation includes, but is not limited to: Social Security numbers, driver's license numbers, U.S. passport numbers, medical information, and health insurance information.

21. Based on Defendants' violation of the CCPA as described herein, Plaintiff and all similarly situated persons therefore are entitled to bring a private action pursuant to California Civil Code Section 1798.150(a). PARKER-HANNIFIN's failure to adequately protect the nonpublic Personal Information and Medical Information in their possession has likely caused, and will continue to cause, substantial harm and injuries to Plaintiff and Class members. Plaintiff and all other similarly situated individuals face a long-term battle against identity theft if their full names, Social Security numbers, dates

of birth, addresses, drivers' license and passport numbers and other sensitive personal and financial information were contained in this unauthorized access and exfiltration. Plaintiff and the Class members have a continuing interest in ensuring that their information is and remains safe.

22. As shown by PARKER-HANNIFIN's total shutdown of certain systems in response to this cyber event, Defendants' unlawful conduct presents an imminent and impending continuing risk for Plaintiff and Class members, particularly where PARKER-HANNIFIN refuses to disclose any of the details about the ransomware attack – including that this data is now accessible on the dark web. As a result of Defendants' conduct and the ensuing Data Breach, Plaintiff and the members of the proposed Class have suffered damages, and are additionally at imminent risk of future harm, including identity theft and fraud.

Accordingly, Plaintiff brings this action on behalf of himself and Class of all others similarly situated and for the benefit of the general public, to seek redress for Defendants' unlawful conduct. Plaintiff and the Class are thus entitled to injunctive relief, legal equitable relief, damages, costs and expenses of litigation, and attorneys' fees.

JURISDICTION AND VENUE

23. This Court has original jurisdiction over this action under 28 U.S.C. § 1332(d) because the amount in controversy exceeds the sum of $5,000,000, exclusive of interest and costs, and is a class action in which at least one member of the Class (as defined below) is a citizen of a State different from Defendants.

24. Venue is appropriate in this District under 28 U.S.C. § 1391 because a substantial part of the events or omissions giving rise to the claim occurred in this District, and Plaintiff and other class members reside in this District.

PARTIES

25. On personal knowledge, Plaintiff John Doe is a citizen and current resident of the State of California. Plaintiff, in the course of his employment with PARKER-HANNIFIN or a subsidiary thereof, was required to provide sensitive Personal Information, including his Social Security number, driver's license, passport number and banking information. Plaintiff was also a former enrollee of PARKER-HANNIFIN's Group Health Plan, and in connection therewith also provided Defendants with

individually identifiable information and Medical Information, as defined by Civil Code section 56.05(i). While Defendant has yet to provide the particulars, it is likely some amount of Plaintiff's Medical Information was created, maintained, preserved, and stored onto Defendant's computer network. Such Medical Information included or contained an element of personal identifying information sufficient to allow identification of the individual, such as name, date of birth, address, and Social Security number, and additionally likely also contained medical record number, insurance provider, electronic mail address, telephone number, or other information that, alone or in combination with other publicly available information, reveals Plaintiff's identity. Given the highly sensitive nature of the information stolen in the Data Breach, Plaintiff remains at a substantial and imminent risk of future harm, including identity theft and theft from his bank accounts. Plaintiff has expended and will be required to expend time and effort monitoring his financial accounts and credit reports. Through the exfiltration of such data, he has been injured in fact and lost money or property as a result of Defendants' misconduct in having his Personal Information and/or Medical Information likely disclosed to and stolen by third parties without his authorization, and the confidentiality and integrity of his Medical Information breached, lost, not preserved, and not protected. Plaintiff has also experienced fear, anxiety, and worry caused by the unauthorized disclosure of Personal Information and Medical Information by PARKER-HANNIFIN since he became aware of it and received a letter from PARKER-HANNIFIN offering limited credit monitoring services.

26. Defendant Parker-Hannifin Corporation is an Ohio Corporation, with offices located around the United States, including in this District.

27. The true names, roles, and capacities in terms of their involvement in the wrongdoing at issue, whether individual, corporate, associate, or otherwise, of Defendants named as DOES 1 through 10, inclusive, are currently unknown to Plaintiff and, therefore, are named as Defendants under fictitious names. Plaintiff will identify these Defendants' true identities and their involvement in the wrongdoing at issue if and when they become known.

28. Defendants' conduct described herein, including reviewing, approving, or ratifying the conduct at issue, was undertaken either directly by PARKER-HANNIFIN or as an agent, servant, contractor, or employee of PARKER-HANNIFIN, and/or was performed within the course and scope of

their authority, agency, or employment. Defendants are thus jointly and severally responsible, in whole or in part, for the conduct, damages, and injuries alleged herein.

FACTUAL ALLEGATIONS

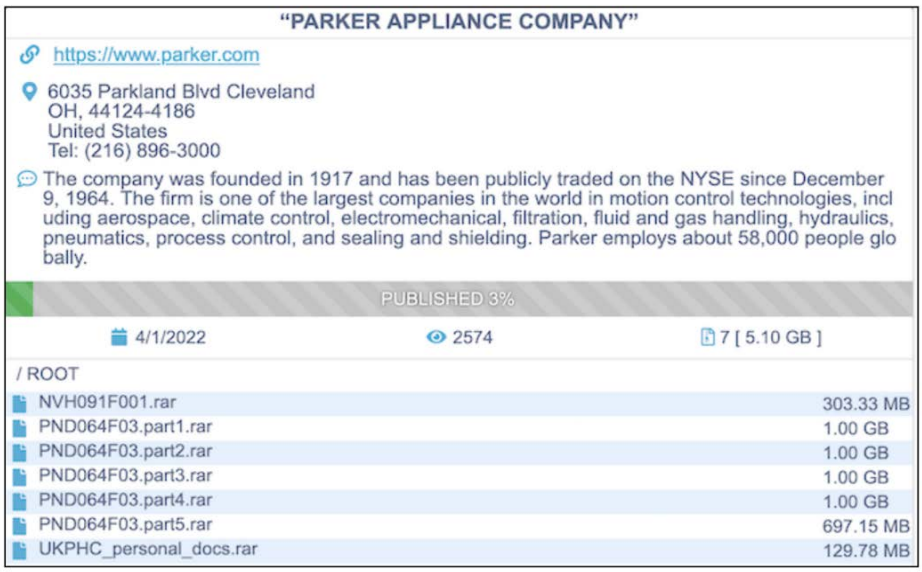
A. THE NATURE OF THE RANSOMWARE ATTACK.

29. On or about May 12, 2022, PARKER-HANNIFIN reported a data breach affecting almost 120,000 current and former employees, their dependents, and others, both of PARKER-HANNIFIN and numerous of its subsidiaries.

30. In addition, current or former enrollees of PARKER-HANNIFIN's Group Health Plan (or a health plan sponsored by an entity acquired by PARKER-HANNIFIN), may also have been subject to unauthorized access and theft.

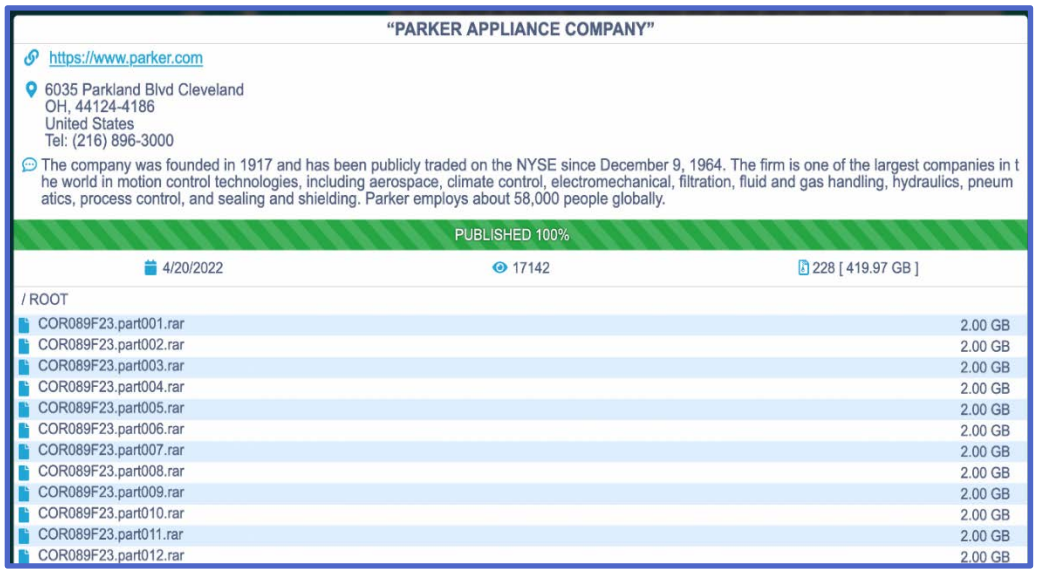
31. PARKER-HANNIFIN's public statement about this data breach and ransomware attack was first disclosed in a Form 8-K filed with the Securities and Exchange Commission on or about April 5, 2022, which stated that "a third party gained unauthorized access to the Company's systems" from March 11-14, 2022. PARKER-HANNIFIN's filing also stated that "the Company believes some data was accessed and taken and may include personal information of Company team members." PARKER-HANNIFIN did not begin notifying affected individuals until on or about May 13, 2022, two months after the Data Breach.

32. While not included in PARKER-HANNIFIN's public statements about this incident, *Security Week* reports that Parker's attack was perpetrated by the Conti ransomware group. On or about April 1, 2022 the Conti group published 5 GB of the stolen files on the dark web, which purportedly was only 3% of the data taken.



screenshot of the Conti data leak page published by Security Week (https://www.securityweek.com/ransomware-gang-leaks-files-stolen-industrial-giant-parker-hannifin)

Typically, this sort of publication is initially done to prove the personal data has been successfully stolen.



(*screenshot of the Conti data leak page for PARKER-HANNIFIN as of May 19, 2022)*

33. On or about April 20, 2022, Conti announced through its data leak page that 100% of the data taken from PARKER-HANNIFIN has been published. The size of the data purportedly released to the dark web for open access is 419.97 GB. It further appears that this data leak page has been publicly viewed and accessed over 17,000 times.

34. According to a report recently filed with the U.S. Department of Health and Human

Services, PARKER-HANNIFIN has reported that 119,513 people are impacted by the Data Breach.

35. The Conti ransomware group accessed and exfiltrated this data with the intent to misuse it, including to demand ransom, marketing and/or selling this information on the dark web.

36. The only clue PARKER-HANNIFIN provided that it had been subject to a ransomware attack and had Personal Information and Medical Information of over 100,000 employees stolen from its servers was that it told individuals, in a notice sent on or about May 12, 2022, that an unauthorized person had gained access to its IT servers. Despite its duties and obligations under California law to promptly provide notice to consumers of such material facts so that they could take appropriate action, PARKER-HANNIFIN did not inform members for two months that an unauthorized party accessed and may have acquired certain files on PARKER-HANNIFIN's IT systems that contain information pertaining to a significant number of current and former PARKER-HANNIFIN employees, their dependents, and other individuals affiliated with the company or its subsidiaries. To date, PARKER-HANNIFIN has never disclosed that it was the subject of a ransomware attack, that its systems had been encrypted by the Conti ransomware group, whether or not it paid the ransom, and that all of this Medical Information, Personal Information and personal financial information had been stolen and was disclosed on the internet.

B. PARKER-HANNIFIN WAS ON NOTICE OF THE POTENTIAL FOR THIS ATTACK.

37. PARKER-HANNIFIN has been on notice for almost a year of the potential for a Conti ransomware attack on its systems but did not take sufficient steps to prevent it.

38. PARKER-HANNIFIN's negligence in safeguarding the Medical Information, Personal Information and personal financial information of Plaintiff and the Class members was exacerbated by the repeated warnings and alerts directed to U.S. companies, warning that they should protect and secure sensitive data, especially in light of the substantial increase in cyberattacks by the Conti ransomware group.

39. The FBI has been warning companies such as PARKER-HANNIFIN about the threat posed by the Conti ransomware group, and to be on the lookout for attacks from this group, for a year. It issued a Flash Alert about Conti ransomware attacks in May, 2021, and a Joint Cybersecurity Advisory on September 22, 2021, which was updated most recently on March 9, 2022 – *two days before this attack*

took place. The Advisory was disseminated with details about what red flags indicate a business has been compromised by Conti ransomware, and how attacks can be avoided.

40. Specifically, as early as May 20, 2021, the FBI issued a Flash Alert that detailed the threat posed by the Conti group. It highlighted that "among the more than 400 organizations worldwide victimized by Conti, over 290 of which are located in the U.S. Like most ransomware variants, Conti typically steals victims' files and encrypts the servers and workstations in an effort to force a ransom payment from the victim. The ransom letter instructs victims to contact the actors through an online portal to complete the transaction. If the ransom is not paid, the stolen data is sold or published to a public site controlled by the Conti actors."[8]

41. In the initial FBI Flash Alert, the FBI included a lengthy list of recommended mitigations businesses should take in order to avoid or minimize the effects of a Conti attack, including:

- Regularly back up data, air gap, and password protect backup copies offline. Ensure copies of critical data are not accessible for modification or deletion from the system where the data resides.
- Implement network segmentation.
- Implement a recovery plan to maintain and retain multiple copies of sensitive or proprietary data and servers in a physically separate, segmented, secure location (i.e., hard drive, storage device, the cloud).
- Install updates/patch operating systems, software, and firmware as soon as they are released.
- Use multifactor authentication where possible.
- Use strong passwords and regularly change passwords to network systems and accounts, implementing the shortest acceptable timeframe for password changes. Avoid reusing passwords for multiple accounts.
- Disable unused remote access/RDP ports and monitor remote access/RDP logs.
- Require administrator credentials to install software.

[8] FBI Flash: Conti Ransomware Attacks Impact Healthcare and First Responder Networks (May 20, 2021); https://www.ic3.gov/Media/News/2021/210521.pdf.

- Audit user accounts with administrative privileges and configure access controls with least privilege in mind.
- Install and regularly update anti-virus and anti-malware software on all hosts.
- Only use secure networks and avoid using public Wi-Fi networks. Consider installing and using a VPN.
- Consider adding an email banner to messages coming from outside your organizations.
- Disable hyperlinks in received emails.
- Focus on cyber security awareness and training.
- Regularly provide users with training on information security principles and techniques as well as overall emerging cybersecurity risks and vulnerabilities (i.e., ransomware and phishing scams).[9]

42. On September 22, 2021, in continuing efforts to alert businesses and their employees about the growing Conti threat, the FBI and NSA sent out warning about the Conti group over Twitter,

[9] *Id.*

with a call to take "immediate action." (tweet from @NSACyber last accessed May 19, 2022 below).

43. On that same day, September 22, 2021, the U.S. Cybersecurity & Infrastructure Security Agency ("CISA"), in conjunction with the FBI and NSA published a Joint Cybersecurity Advisory on Conti Ransomware.[10]

44. In that Joint Cybersecurity Advisory, CISA provided businesses with a lengthy listing of technical details that explained how the group was gaining initial access to business IT networks, indicators that would let businesses know they had been compromised, techniques used by Conti to compromise IT systems, and yet again, another list of recommended mitigations to reduce the risk of compromise from Conti ransomware attacks, with additional mitigations not previously included in the FBI Flash Alert.[11] The 10-page technical treatise also provided references to other helpful materials for businesses with links, and an offer for "Free Cyber Hygiene Services" offered by CISA to help organizations "assess, identify, and reduce their exposure to threats, including ransomware."[12] The increase in such attacks, and the attendant risk of future attacks, was widely known within PARKER-HANNIFIN's business community. Due to the high-profile nature of these breaches and attacks, Defendants either were or should have been on heightened notice and aware of such attacks and, therefore, should have been on notice of their duty to be proactive in guarding against being subject to such attacks and adequately performed their duty of preparing for and immediately identifying such an attack.

45. Yet despite the prevalence of public announcements of these data breach and data security compromises and despite numerous attempts on the part of the federal government to inform government contractor companies like PARKER-HANNIFIN of the threat posed by ransomware attacks in general and Conti in particular, and despite having almost a year from their attack to prepare and prevent such an attack, PARKER-HANNIFIN was negligent and did not adequately prepare for this wholly foreseeable event, allowing extremely sensitive data to be accessed, viewed and stolen by the Conti ransomware group. Defendants thus breached their duty to take appropriate steps to protect Plaintiff's

[10] *See,* Joint Cybersecurity Advisory: Conti Ransomware (9/22/21); https://www.cisa.gov/uscert/sites/default/files/publications/AA21-265A-Conti_Ransomware_TLP_WHITE.pdf (last accessed May 24, 2022).
[11] *Id.*
[12] *Id.* page, 9.

and Class members' Personal Information and/or Medical Information from being compromised and have failed to adequately notify such persons that such a ransomware attack has taken place.

46. Unfortunately for Plaintiff and other similarly situated individuals, their Personal Information and Medical Information was not secured in the manner required under California law that would have prevented this Conti attack. What's worse, despite Defendants' obligations under the law to promptly notify affected individuals so they can take appropriate action, Defendants failed to promptly provide such notice in the most expedient time possible and without unreasonable delay, failed to include in the data breach notice a sufficient description of the data breach incident to comply with Civil Code Section 1798.29(d)(2)(E), and any other relevant laws, and failed to provide in the Data Breach notice the information needed by Plaintiff and other similarly situated individuals to enable them react appropriately to the breach, including taking whatever mitigation measures are necessary.

47. As a result, this unauthorized access, disclosure, and exfiltration remains unremedied. Defendants have failed to provide notice to affected consumers in the most expedient time possible and without unreasonable delay, as required under California law.

C. DEFENDANTS HAD AN OBLIGATION TO PROTECT PERSONAL AND MEDICAL INFORMATION UNDER STATE AND FEDERAL LAW AND THE APPLICABLE STANDARD OF CARE.

48. Defendants are required by the CCPA, the CMIA and various other laws and regulations to protect Plaintiff's and Class members' Personal Information and Medical Information and to handle notification of any breach in accordance with applicable breach notification statutes. Failing to do so results in acts of negligence *per se* by Defendants. These duties are established in numerous California statutes, including California Civil Code Sections 56.101, 1798.150(a) and 1798.82.

49. In addition, as federal government contractors, Defendants made representations that they would comply with numerous cybersecurity requirements applicable to the protection of data on their computer systems, including but not limited to Federal Acquisition Regulation 52.204-21 and Defense Federal Acquisition Regulation Supplement 252.204-7012, which impose physical and cybersecurity obligations on contractor systems that process government information.

50. In addition, to the extent that PHI was affected by the Data Breach, as Defendants may be entities covered by the Health Insurance Portability and Accountability Act ("HIPAA") (45 C.F.R. §

160.102) they are required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C, which establish national security standards and duties for Defendants' protection of Medical Information maintained by them in electronic form.

51. HIPAA requires Defendants to "comply with the applicable standards, implementation specifications, and requirements" of HIPAA "with respect to electronic protected health information." 45 C.F.R. § 164.302.

52. "Electronic protected health information" is defined as "individually identifiable health information ... that is (i) transmitted by electronic media; maintained in electronic media." 45 C.F.R. § 160.103.

53. HIPAA's Security Rule requires Defendants to: (a) ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits; (b) protect against any reasonably anticipated threats or hazards to the security or integrity of such information; (c) protect against any reasonably anticipated uses or disclosures of such information that are not permitted; and (d) ensure compliance by their workforce.

54. HIPAA also requires Defendants to "review and modify the security measures implemented ... as needed to continue provision of reasonable and appropriate protection of electronic protected health information," 45 C.F.R. § 164.306(c), and also to "[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights." 45 C.F.R. § 164.312(a)(1).

55. The ransomware attack on Defendants, particularly in light of the information received by them almost a year before the attack, establishes they did not comply with these Rules. This attack resulted from a combination of inadequacies that demonstrate Defendants failed to comply with safeguards mandated by HIPAA regulations, including, but not limited to, the following:

(a) Failing to ensure the confidentiality and integrity of electronic PHI that Defendants

create, receive, maintain, and transmit, in violation of 45 C.F.R. section 164.306(a)(1);

(b) Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights, in violation of 45 C.F.R. section 164.312(a)(1);

(c) Failing to implement policies and procedures to prevent, detect, contain, and correct security violations, in violation of 45 C.F.R. section 164.308(a)(1);

(d) Failing to identify and respond to suspected or known security incidents and mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity, in violation of 45 C.F.R. section 164.308(a)(6)(ii);

(e) Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic PHI, in violation of 45 C.F.R. section 164.306(a)(2);

(f) Failing to protect against any reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information, in violation of 45 C.F.R. section 164.306(a)(3);

(g) Failing to ensure compliance with HIPAA security standard rules by its workforce, in violation of 45 C.F.R. section 164.306(a)(4);

(h) Impermissibly and improperly using and disclosing PHI that is and remains accessible to unauthorized persons, in violation of 45 C.F.R. section 164.502, *et seq.*;

(i) Failing to effectively train all members of its workforce (including independent contractors) on the policies and procedures with respect to PHI as necessary and appropriate for the members of its workforce to carry out their functions and to maintain security of PHI, in violation of 45 C.F.R. sections 164.530(b) and 164.308(a)(5); and

(j) Failing to design, implement, and enforce policies and procedures establishing

physical and administrative safeguards to reasonably safeguard PHI in compliance with 45 C.F.R. section 164.530(c).

56. Defendants also violated the duties applicable to them under the Federal Trade Commission Act (15 U.S.C. § 45 *et seq*.) from engaging in "unfair or deceptive acts or practices in or affecting commerce." The FTC pursuant to that Act has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act.[13]

57. As established by these laws, Defendants owed a duty to Plaintiff and Class members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Medical Information in their possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendants also owed a duty to Plaintiff and Class members to provide reasonable security in compliance with industry standards and state and federal requirements, and to ensure that their computer systems, networks, and protocols adequately protected this Medical Information and were not exposed to infiltration. This also included a duty to Plaintiff and the Class members to design, maintain, and test their computer systems to ensure that the Personal Information and Medical Information in their possession was adequately secured and protected; to create and implement reasonable data security practices and procedures to protect the Personal Information and Medical Information in their possession and avoid access to their systems through processes such as phishing, including adequately training employees and others who accessed information within their systems on how to adequately protect the Personal Information and Medical Information and avoid permitting such infiltration such as by use of multi-factor authentication; to implement processes that would detect a breach of their data security systems in a timely manner and to act upon data security warnings and alerts in a timely fashion; to disclose if their computer systems and data security practices were inadequate to safeguard individuals' Personal Information and Medical Information from theft; and to disclose in a timely and accurate manner when data breaches or ransomware attacks occurred. Defendants also needed to segment data by, among other things, creating firewalls and access controls so that if one area of Defendants' network is compromised, hackers cannot gain access to other portions of Defendants' systems.

[13] *See, e.g., FTC v. Wyndham Worldwide Corp.*, (3d Cir. 2015) 799 F.3d 236.

58. Defendants owed these duties to Plaintiff and Class members because they were foreseeable and probable victims of any inadequate data security practices. Defendants affirmatively chose to design their systems with inadequate user authentication, security protocols and privileges, and set up faulty patching and updating protocols. These affirmative decisions resulted in Conti being able to execute the ransomware attack and exfiltrate the data in question, to the injury and detriment of Plaintiff and Class members. By taking affirmative acts inconsistent with these obligations that left PARKER-HANNIFIN's computer system vulnerable to a ransomware attack, Defendants disclosed and/or permitted the disclosure of Personal Information and Medical Information to unauthorized third parties. Through such actions or inactions, PARKER-HANNIFIN failed to preserve the confidentiality of various pieces of Personal Information and Medical Information they were duty-bound to protect.

59. As a direct and proximate result of Defendants' actions, inactions, omissions, breaches of duties and want of ordinary care that directly and proximately caused or resulted in the ransomware attack and the resulting data breach, Plaintiff and Class members have suffered and will continue to suffer damages and other injury and harm not fully compensable by the payment of damages in the form of, *inter alia*, (a) present, imminent, immediate and continuing increased risk of identity theft, identity fraud and medical fraud -- risks justifying expenditures for protective and remedial services for which they are entitled to compensation, (b) invasion of privacy, (c) breach of the confidentiality of their Personal Information and Medical Information, (d) deprivation of the value of their Personal Information and Medical Information, for which there is a well-established national and international market, as well as statutory damages to which they are entitled even without proof of access or actual damages; (e) the financial and temporal cost of monitoring their credit reports, (f) increased risk of future harm, and/or (g) fear, anxiety, and worry caused by the unauthorized release of their Personal Information and Medical Information, all resulting in a loss of money or property related to Defendants' misconduct.

D. THE VALUE OF PERSONAL INFORMATION AND MEDICAL INFORMATION SHOWS THAT PLAINTIFF AND OTHERS LOST VALUABLE MONEY OR PROPERTY AS A RESULT OF THIS ATTACK AND DO NOT HAVE AN ADEQUATE REMEDY AT LAW.

60. It is well known that Personal Information and Medical Information is a valuable commodity[14] and the frequent target of hackers, such that Plaintiff and Class members would lose money or property if their data was permitted to be improperly accessed or stolen and that they would not have an adequate remedy at law simply by receiving payment for damages and limited credit monitoring.

61. The unauthorized disclosure of Social Security numbers can be particularly damaging because Social Security numbers cannot easily be replaced. In order to obtain a new number, a person must prove, among other things, that he or she continues to be disadvantaged by the misuse. Thus, under current rules, no new number can be obtained until damage has been done. Furthermore, as the Social Security Administration warns: "A new number probably will not solve all your problems. This is because other governmental agencies (such as the Internal Revenue Service and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) likely will have records under your old number. Also, because credit reporting companies use the number, along with other Personal Information, to identify your credit record, using a new number will not guarantee you a fresh start. This is especially true if your other Personal Information, such as your name and address, remains the same. If you receive a new Social Security Number, you will not be able to use the old number anymore." Social Security Administration, Identity Theft and Your Social Security Number (June 2017), available at http://www.ssa.gov/pubs/10064.html (last visited Nov. 22, 2019).

62. For some victims of identity theft, a new Social Security number actually creates new problems. If the old credit card information is not associated with the new number, the absence of any credit history under the new number may make it more difficult for you to get credit.

63. According to the Attorney General of the United States, Social Security numbers "can be an identity thief's most valuable piece of consumer information." Fact Sheet: The Work of the President's Identity Theft Task Force, DOJ 06-636, 2006 WL 2679771 (Sep. 19, 2006). Indeed,: "The ubiquity of

[14] See, e.g., John T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

the SSN as an identifier makes it a primary target for both hackers and identity thieves. . . . When data breaches expose SSNs, thieves can use these numbers—usually combined with other pieces of data—to impersonate individuals and apply for loans, housing, utilities, or government benefits. Additionally, this information may be sold on the black market to other hackers." Daniel J. Marcus, The Data Breach Dilemma: Proactive Solutions for Protecting Consumers' Personal Information, 68 Duke L.J. 555, 564–65 (2018).

64. Defendants either were or should have been aware that the Personal Information, Medical Information, PII and PHI they collected and retained is highly sensitive and of significant value to those who would use it for wrongful purposes months if not years after the breach took place. As the FTC has reported, identity thieves can use this information to commit an array of crimes including identify theft, medical and financial fraud.[15] Medical identity theft is one of the most common, most expensive, and most difficult-to-prevent forms of identity theft.

65. Indeed, a robust cyber black market exists in which criminals post stolen Medical Information, PII and PHI on multiple underground Internet websites, commonly referred to as the dark web, to create fake insurance claims, purchase and resell medical equipment, or access prescriptions for illegal use or resale. According to a 2017 Javelin strategy and research presentation, fraudulent activities based on data stolen in data breaches that is between two and six years old had increased by nearly 400% over the previous four years.[16] Thus, an offer of credit monitoring service that is only for two years is not an adequate remedy or offer, even if it conducts dark web scanning (which is unclear here).

66. According to Experian, one of the three major credit bureaus, medical records can be worth up to $1,000 per person on the dark web, depending upon completeness.[17] PII and PHI can be sold at a price ranging from approximately $20 to $300.[18]

67. In this case, all evidence indicates that Plaintiff and Class Members' Personal Information and Medical Information were left unprotected, to be freely accessed on the dark web by the Conti group

[15] Federal Trade Commission, What To Know About Identity Theft, https://consumer.ftc.gov/articles/what-know-about-identity-theft (last accessed 5/3/22).
[16] *See*, Brian Stack, *Here's How Much Your Personal Information is Selling for on the Dark Web* (2017) https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last accessed 5/23/22).
[17] *Id.*
[18] https://www.privacyaffairs.com/dark-web-price-index-2021/

after exfiltration. Thus, this highly valuable data was left to be pilfered by criminals or reviewed by anyone with an Internet connection – and has been accessed at least 17,000 times already.

68. Medical identify theft can also result in inaccuracies in medical records and costly false claims. It can also have life-threatening consequences since if a victim's health information is mixed with other records, it can lead to misdiagnosis or mistreatment. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."[19]

69. The Ponemon Institute found that medical identity theft can cost victims an average of $13,500 to resolve per incident, and that victims often have to pay off the imposter's medical bills to resolve the breach.[20]

70. In another study by the Ponemon Institute in 2015, 31% of medical identity theft victims lost their healthcare coverage as a result of the incident, while 29% had to pay to restore their health coverage, and over half were unable to resolve the identity theft at all.[21]

71. Once Personal Information and Medical Information is stolen, particularly such as membership identification numbers or Social Security numbers, fraudulent use of that information and damage to victims may continue for years, as the fraudulent use of such data resulting from the attack may not come to light for years. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches: "[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue

[19] Michael Ollove, "The Rise of Medical Identity Theft in Healthcare," Kaiser Health News, (2/7/14), https://khn.org/news/rise-of-indentity-theft/ (last accessed 5/3/22); *See also*, *Medical Identity Theft in the New Age of Virtual Healthcare*, IDX (March 15, 2021), https://www.idx.us/knowledge-center/medical-identity-theft-in-the-new-age-of-virtual-healthcare (last accessed 5/3/22).
[20] Brian O'Connor, Healthcare Data Breach: What to Know About Them and What to Do After One, Experian (June 14, 2018), https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-know-about-them-and-what-to-do-after-one/ (last accessed 5/3/22).
[21] Ponemon Institute, *Fifth Annual Study on Medical Identity Theft*, (February, 2015), http://www.medidfraud.org/wp-content/uploads/2015/02/2014_Medical_ID_Theft_Study1.pdf (last accessed 5/3/22).

for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm."[22]

72. The ramifications of Defendants' failure to keep the Personal Information and Medical Information in question secure from attack and then not advise affected persons of all the relevant facts is thus not temporary but long lasting, as the fraudulent use of that information and damage to victims may continue for years, and long after the expiration of any offered credit monitoring services. Criminals often trade stolen medical information, PII and PHI on the "cyber black market" for years following a breach. For example, it is believed that certain PHI/PII compromised in the 2017 Experian data breach was being used three years later by identity thieves to apply for COVID-19-related benefits.[23] That is one of the reasons providing prompt notice to consumers as expeditiously as possible is necessary, so they can take actions to protect themselves. Yet Defendants are still refusing to even acknowledge that a ransomware and resulting data breach took place, let alone provided comprehensive notice in the most expedient time possible and without unreasonable delay, as required under California law.

73. For all these reasons, Plaintiff and Class members thus have no other adequate remedy at law since the payment of actual and statutory damages will not adequately address these realities. Absent injunctive relief from the Court Defendants are likely to not fully redress the issues raised by their illegal and unfair business practices. Defendants have not announced any specific changes to their data security infrastructure, processes, or procedures to fix the vulnerabilities in the electronic information security systems and/or security practices that permitted the Conti ransomware attack and the Data Breach to occur and go undetected, and thereby prevent further attacks, nor did they provide complete and prompt notice of the circumstances surrounding this breach as required by law.

CLASS ALLEGATIONS

74. Plaintiff, on behalf of himself and all others similarly situated, brings this action pursuant

[22] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO, July 5, 2007, https://www.govinfo.gov/content/pkg/GAOREPORTS-GAO-07-737/html/GAOREPORTS-GAO-07-737.htm (last accessed 5/3/22).

[23] Janelle Stecklein, *Director: 64,000-plus fraudulent unemployment claims'mitigated'*, The Duncan Banner (June 24, 2020), https://www.duncanbanner.com/news/director-64-000-plus-fraudulent-unemployment-claims-mitigated/article_dc446671-73a6-5e8a-b732-bcedba72b458.html (last accessed 5/3/22)

to Fed R. Civ. Proc. 23. This action satisfies the numerosity, commonality, typicality, adequacy, predominance, and superiority requirements for class certification.

75. The proposed class ("Class") is defined as:

> All current California residents who are present or former employees of PARKER-HANNIFIN or one of its subsidiaries and whose information was accessed and released or disclosed as a result of the Conti ransomware attack in or about March, 2022.
>
> The Class also contains a sub-Class ("the Medical Information Sub-class") that consists of all persons who fall within the definition of the Class whose Medical Information was accessed and released or disclosed as a result of the Conti ransomware attack in or about March, 2022.

76. Plaintiff reserves the right to modify or amend the definition of the proposed Class before the Court determines whether class certification is appropriate.

77. The members of the Class are sufficiently numerous such that joinder of all Class members is impracticable. The proposed Class contains past or current PARKER-HANNIFIN or subsidiary employees, certain of their dependents, and certain members of PARKER-HANNIFIN's group health plans or a health plan sponsored by an entity acquired by PARKER-HANNIFIN that, according to a recent filing with the HHS Office of Civil Rights, consists of 119,513 individuals.

78. Common questions of law and fact exist as to all members of the Class and predominate over questions affecting only individual Class members. The factual bases underlying Defendants' misconduct is common to all Class members and represents a common thread of unlawful and negligent conduct, resulting in injury to all members of the Class. These common legal and factual questions include the following:

(a) Whether Defendants implemented and maintained reasonable security practices and procedures appropriate to protect Plaintiff's and Class members' Personal Information and Medical Information from unauthorized access, use, theft, modification, or disclosure;

(b) Whether Defendants and their employees, agents, officers, and/or directors negligently and/or unlawfully disclosed or permitted the unauthorized disclosure of Plaintiff's and Class members' Personal Information and Medical Information to unauthorized persons;

(c) Whether Defendants negligently created, maintained, preserved, stored, abandoned, or disposed of Plaintiff's and Class members' Personal Information and Medical Information, and failed to

protect and preserve the integrity of the Personal Information and Medical Information found on PARKER-HANNIFIN's computer systems;

(d) Whether Defendants' actions or inactions were a proximate result of the negligent release of confidential information or records concerning Plaintiff and members of the Class;

(e) Whether Defendants adequately, promptly, timely and accurately informed Plaintiff and the Class members that their Personal Information and Medical Information had been compromised and whether Defendants violated the law by failing to promptly notify Plaintiff and the Class members of this material fact;

(f) Whether Defendants have adequately addressed and fixed the vulnerabilities in their computer system that permitted the ransomware attack and resulting data breach to occur;

(g) Whether Defendants engaged in "unfair" business practices by failing to safeguard the Personal Information and Medical Information of Plaintiff and the Class, and whether Defendants' violations of the state and federal laws cited herein constitute "unlawful" business practices in violation of California Business and Professions Code § 17200, et seq.;

(h) Whether Defendants violated California's CCPA, CMIA and the other laws cited herein; and

(i) Whether Plaintiff and the Class are entitled to damages, equitable relief and/or injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Conti ransomware attack and Defendants' failure to provide notice thereof, and the scope of such relief.

79. Plaintiff's claims are typical of the claims of other Class members. There is no unique defense available to Defendants as Plaintiff, like all Class members, was a PARKER-HANNIFIN employee, was enrolled in PARKER-HANNIFIN's health services plan and was apparently subjected to the unauthorized disclosure of Personal Information and Medical Information as a result of Defendants' conduct.

80. Plaintiff will fairly and adequately represent the interests of the Class members. Plaintiff has retained counsel with substantial experience in prosecuting complex litigation and class actions, including data breaches concerning the sensitive Personal Information and Medical Information of individuals. Plaintiff and his counsel are committed to vigorously prosecuting the action on behalf of the

Class. Neither Plaintiff nor his counsel has any interest adverse to or that irreconcilably conflicts with those of other Class members.

81. Absent a class action, most members of the Class would find the cost of litigating their claims to be prohibitive and may have no effective and complete remedy. Class treatment of common questions of law and fact is also superior to multiple individual actions or piecemeal litigation and results in substantial benefits in that it conserves the resources of the courts and litigants and promotes consistency and efficiency of adjudication. The conduct of this action as a class action presents few management difficulties and protects the rights of each Class member. Plaintiff thus anticipates no difficulty in the management of this case as a class action and providing notice to members of the Class.

82. Class treatment is also appropriate because Defendants have acted on grounds generally applicable to members of the Class, making class-wide equitable, injunctive, and declaratory relief appropriate.

CAUSES OF ACTION

FIRST CAUSE OF ACTION

Violation of the California Consumer Privacy Act

Cal. Civ. Code § 1798.100 *et seq*.

83. Plaintiff incorporates the foregoing allegations as if fully set forth herein. This count is brought on behalf of the Class and the Sub-Class. Plaintiff does not assert a claim for damages at this time under this Cause of Action and does not incorporate by reference any allegations pertaining to requests for damages.

84. The CCPA was enacted to protect consumers' sensitive information from collection and use by businesses without appropriate notice and consent.

85. Through the above-detailed conduct, Defendant violated CCPA by subjecting the nonencrypted and nonredacted Personal Information of Plaintiff and Class members to unauthorized access, theft, or disclosure as a result of Defendant's violation of its duty to implement and maintain reasonable security procedures and practices appropriate to the nature and protection of that information. Cal. Civ. Code § 1798.150(a).In accordance with Cal. Civ. Code § 1798.150(b), Plaintiff's counsel has sent a Notice of Violation to PARKER-HANNIFIN on behalf of Plaintiff and all other similarly situated

California residents. Plaintiff does not assert claims for damages at this time for his claim under the CCPA, but reserves the right to do so if Defendants do not timely respond to and accept Plaintiff's claim for damages, on behalf of both himself and all others similarly situated.

86. On behalf of Class members, Plaintiff seeks injunctive relief in the form of an order enjoining Defendant from continuing to violate the CCPA. If Defendant fails to timely respond to Plaintiff's notice letter or agree to rectify the violations detailed above, Plaintiff also will seek actual and punitive damages, Plaintiff will also seek statutory damages of between $100 and $750 per Class member, attorneys' fees and costs, and any other relief the Court deems proper as a result of Defendant's CCPA violations.

SECOND CAUSE OF ACTION

Violation of the Confidentiality of Medical Information Act

Cal. Civ. Code § 56 *et seq*.

87. Plaintiff incorporates the foregoing allegations by reference as if fully set forth herein. The Cause of Action is brought on behalf of the Medical Information Sub-class.

88. PARKER-HANNIFIN is subject to the requirements of the CMIA as an employer under Cal. Civ. Code Section 56.20(a) and as a corporation that receives Medical Information regarding a patient under California Civil Code Section 56.10(e), which as noted above it admits to having received.

89. PARKER-HANNIFIN must not disclose or permit the disclosure of Medical Information regarding a patient of the provider of health care or an enrollee or subscriber of a health care service plan without first obtaining authorization, subject to certain exceptions found in Civil Code Section 56.10(b) & (c) that do not apply here. (Cal. Civ. Code §§ 56.10(a) & (e).) Further, to the extent the PARKER-HANNIFIN was an employer of Plaintiff and Class members, it is prohibited from using disclosing, or knowingly permitting its employees or agents to use or disclose Medical Information that PARKER-HANNIFIN possesses pertaining to its employees without the patient having first signed an authorization, except under certain exceptions not relevant to this action. Additionally, to the extent the PARKER-HANNIFIN was an employer to Plaintiff and Class members, it was also required to establish appropriate procedures to ensure the confidentiality and protection from unauthorized use and disclosure of Medical Information it has received, including, but not limited to instruction regarding confidentiality to

employees and agents handling files containing Medical Information, and security systems restricting access to files containing Medical Information. By their affirmative acts and inactions set forth above, Defendants disclosed or permitted the disclosure of Medical Information to unauthorized third parties in violation of this Section, as well as failed establish appropriate procedures to ensure the confidentiality and protection from unauthorized use and disclosure of the Medical Information it had received.

90. PARKER-HANNIFIN is required under the CMIA to ensure that it maintains, preserves, and stores Medical Information in a manner that preserves the confidentiality of the information contained therein. (Cal. Civ. Code § 56.101(a) & 56.36(b).)

91. PARKER-HANNIFIN is required to create, maintain, preserve, store, abandon, destroy or dispose of Medical Information in a non-negligent manner. (Cal. Civ. Code § 56.101(a).)

92. Under the CMIA, electronic health record systems or electronic medical record systems are required to protect and preserve the integrity of electronic Medical Information. (Cal. Civ. Code § 56.101(b)(1)(A).) The term "electronic health record" or "electronic medical record" means an electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff. (Cal. Civ. Code § 56.101(c) as defined by 42 U.S.C. § 17921(5).)

93. Plaintiff and members of the Class are "Patients" as defined by Cal. Civ. Code section 56.05(j).

94. The information at issue in this action is "Medical Information" as that term is defined by section 56.05(i) of the CMIA.

95. As described above, the actions or inactions of PARKER-HANNIFIN failed to preserve the confidentiality of Medical Information, including but not limited to Plaintiff's and Class members' Personal and Medical Information. In addition, with respect to current or former enrollees of PARKER-HANNIFIN's Group Health Plan or a health plan sponsored by an entity acquired by PARKER-HANNIFIN, the actions or inactions of PARKER-HANNIFIN failed to preserve the confidentiality of Medical Information, including but not limited to: health plan enrollment information, health insurance plan ID numbers, and dates of coverage, and for a smaller subset of individuals, dates of medical coverage, dates of medical services, provider names, claims information and medical and clinical

treatment information either that, alone or in combination with other publicly available information, reveals their identities.

96. The Medical Information that was the subject of the Conti ransomware attack and resulting data breach detailed above was accessed, removed and viewed by the Conti ransomware group and its members, and other unauthorized parties during and following the ransomware attack.

97. Since the Conti ransomware group published the entirety of the almost 420 gigabytes of data it exfiltrated onto the web to be downloaded freely, the data at issue herein was viewed and the confidentiality and integrity of that data was breached, lost, not preserved, and not protected by Defendants.

98. In violation of the CMIA, Defendants disclosed or permitted the disclosure of Medical Information regarding Plaintiff and Class members without authorization to a third party. This disclosure did not qualify for any of the exemptions set forth in Civil Code Section 56.10(b) or (c), which provide limited bases for allowing unauthorized disclosures. This disclosure of Medical Information to unauthorized individuals resulted from the affirmative actions and inactions of Defendants and their employees, which allowed hackers from the Conti ransomware group to access, view and obtain the Medical Information of tens of thousands of PARKER-HANNIFIN or subsidiary employees or their dependents.

99. In violation of the CMIA, Defendants created, maintained, preserved, stored, abandoned, destroyed, or disposed of Medical Information of Plaintiff and Class members in a manner that did not preserve the confidentiality of the information contained therein.

100. In violation of the CMIA, Defendants negligently created, maintained, preserved, stored, abandoned, destroyed, or disposed of Medical Information of Plaintiff and Class members.

101. In violation of the CMIA, PARKER-HANNIFIN's electronic health record systems or electronic medical record systems did not protect and preserve the integrity of Plaintiff's and Class members' Medical Information.

102. In violation of the CMIA, Defendants negligently released confidential information or records concerning Plaintiff and Class members.

103. In violation of the CMIA, Defendants failed to give prompt, timely and fulsome notice of

the Conti ransomware attack and resulting data breach.

104. As a direct and proximate result of Defendants' wrongful actions, inactions, omissions, and want of ordinary care that directly and proximately caused the release of Medical Information of thousands of individuals, such personal Medical Information was viewed by, released to, and disclosed to third parties without appropriate written authorization.

105. Plaintiff and members of the Medical Information Sub-class are therefore entitled to injunctive relief, actual damages, statutory damages of $1,000 per sub-Class member, punitive damages of $3,000 per sub-Class member, and reasonable attorneys' fees of $1,000 per sub-Class Member and costs.

THIRD CAUSE OF ACTION

Invasion of Privacy

California Constitution, Article I, Section 1

106. Plaintiff incorporates the foregoing allegations by reference as if fully set forth herein.

107. The California Constitution provides: "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possession, and protecting property, and pursuing and obtaining safety, happiness, and privacy." Cal. Const., Art. I., § 1.

108. Plaintiff and Class members had a legitimate expectation of privacy in their Personal Information and Medical Information, and were entitled to the protection of this information against disclosure to unauthorized third parties.

109. Defendants owed a duty to Plaintiff and Class members to keep their Personal Information and Medical Information confidential.

110. Defendants failed to protect and released to unauthorized third parties the non-redacted and non-encrypted Personal Information and Medical Information, of Plaintiff and Class members.

111. Defendants allowed unauthorized and unknown third parties access to and examination of the Personal Information and Medical Information of Plaintiff and Class members by way of Defendants' affirmative actions and negligent failures to protect this information.

112. The unauthorized release to, custody of, and examination by unauthorized third parties of

the Personal Information and Medical Information of Plaintiff and Class members is highly offensive to a reasonable person.

113. The intrusion at issue was into a place or thing, which was private and is entitled to be private. Plaintiff and Class members disclosed their Personal Information and Medical Information to Defendants as part of Plaintiff's and Class members' relationships with Defendants, but privately and with the intention that the Personal Information and Medical Information would be kept confidential and would be protected from unauthorized disclosure. Plaintiff and Class members were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

114. The Conti ransomware attack that resulted from the actions and inactions of Defendants constitutes an intentional interference with the Plaintiff's and Class members' interest in solitude or seclusion, either as to their persons or as to their private affairs or concerns and those of their families, of a kind that would be highly offensive to a reasonable person.

115. Defendants acted with a knowing or negligent state of mind when they permitted the attack described herein to occur, because they either knew or reasonably should have known that their information security practices were inadequate and insufficient to protect again such attacks.

116. Defendants either knew or reasonably should have known that their inadequate and insufficient information security practices would cause injury and harm to Plaintiff and Class members.

117. As a proximate result of the above acts and omissions of Defendants, the Personal Information and Medical Information, of Plaintiff and Class members was disclosed to third parties without authorization, causing Plaintiff and Class members to suffer injuries and damages in an amount according to proof.

118. Unless and until enjoined and restrained by order of this Court, Defendants' wrongful conduct will continue to cause irreparable injury to Plaintiff and the Class, entitling them to seek injunctive relief.

119. This action, if successful, will enforce an important right affecting the public interest and would confer a significant benefit, whether pecuniary or non-pecuniary, for a large class of persons and/or the general public. Private enforcement is necessary and places a disproportionate financial burden on Plaintiff in relation to Plaintiff's stake in the matter. Because this case is brought for the purposes of

enforcing important rights affecting the public interest, Plaintiff also seeks the recovery of attorneys' fees and costs in prosecuting this action against Defendants under Code of Civil Procedure section 1021.5 and other applicable law.

FOURTH CAUSE OF ACTION

Violation of the Unfair Competition Law

Cal. Bus. & Prof. Code § 17200 *et seq.*

120. Plaintiff incorporates the foregoing allegations by reference as if fully set forth herein, except all claims as to entitlement to damages.

121. The acts, misrepresentations, omissions, practices, and non-disclosures of Defendants as alleged herein constituted unlawful and unfair business acts and practices within the meaning of California Business & Professions Code sections 17200, et seq.

122. Defendants engaged in "unlawful" business acts and practices in violation of the California statutes set forth above, including Civil Code sections 56.10(a), 56.10(e), 56.20, 56.101, 1798.100 *et seq*., 1798.21, 1798.29 § 1798.100 *et seq*., and Article I, § 1 of the California Constitution. Defendants acts also violated federal statutes and regulations, including the Federal Trade Commission Act (15 U.S.C. § 45 et seq.), Health Insurance Portability and Accountability Act ("HIPAA") (45 C.F.R. § 160.102), the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C and the other sections identified above. Plaintiff reserves the right to allege other violations of law committed by Defendants that constitute unlawful business acts or practices within the meaning of California Business & Professions Code sections 17200, *et seq*.

123. Defendants have also engaged in "unfair" business acts or practices. There are several tests that determine whether a practice that impacts consumers as compared to competitors is "unfair," examining the practice's impact on the public balanced against the reasons, justifications and motives of Defendants. Defendants' conduct would qualify as "unfair" under any of these standards:

(a) does the practice offend an established public policy, which here are whether the practices at issue offend the policies of protecting consumers' Personal Information and Medical

Information by engaging in illegal practices, as reflected in California law and policy set forth above;

(b) balancing the utility of Defendants' conduct against the gravity of the harm created by that conduct, including whether Defendants' practices caused substantial injury to consumers with little to no countervailing legitimate benefit that could not reasonably have been avoided by the consumers themselves, and causes substantial injury to them; or

(c) is the practice immoral, unethical, oppressive, unscrupulous, unconscionable or substantially injurious to consumers.

124. The harm caused by Defendants' failure to maintain adequate information security procedures and practices, including but not limited to failing to take adequate and reasonable measures to ensure their data systems were protected against unauthorized intrusions, failing to properly and adequately educate and train employees, failing to put into place reasonable or adequately protected computer systems and security practices to safeguard employees' Personal Information and Medical Information, including access restrictions, multi-factor authentication and encryption, failing to have adequate privacy policies and procedures in place that did not preserve the confidentiality of the Personal Information and Medical Information of Plaintiff and the Class members in their possession, failing to timely and accurately disclose the ransomware attack and resulting data breach to Plaintiff and Class members, and failing to protect and preserve confidentiality of Personal Information and Medical Information of Plaintiff and Class members against disclosure and/or release, outweighs the utility of such conduct and such conduct offends public policy, is immoral, unscrupulous, unethical, and offensive, and causes substantial injury to Plaintiff and Class members.

125. Defendants either knew or should have known that PARKER-HANNIFIN's data security and protection practices were inadequate to safeguard the Personal Information and Medical Information of Plaintiff and Class members, deter hackers, and detect a ransomware attack and resulting data breach within a reasonable time, even though the risk of a data breach or theft was highly likely, especially given Defendants had been on notice for almost a year of the potential for a Conti ransomware attack on its systems. The business acts and practices by Defendants for failure to keep confidential medical or personal data protected, encrypted and without sufficient security to be breached by an adverse third

party did not meet all applicable standards of care and vigilance. Thousands of individuals are now prime targets for fraud, extortion, or access to other completely private information that would never have been provided to Defendants if the patients or consumers knew how negligent or reckless Defendants would be in not protecting such deeply personal medical and financial information private.

126. These unlawful and unfair business acts or practices conducted by Defendants have been committed in the past and continue to this day. Defendants have failed to acknowledge the wrongful nature of their actions. Defendants have not timely corrected or publicly issued comprehensive corrective notices to Plaintiff and the Class members and may not have corrected or enacted adequate policies and procedures to protect and preserve the confidentiality of medical and personal identifying information of Plaintiff and the Class in their possession.

127. As set forth above, Plaintiff and/or Class members have been injured in fact and lost money or property as a result of Defendants' unlawful and unfair business practices, having lost control over information about them that has a specific inherent monetary value that can be sold, bartered or exchanged.

128. Plaintiff and Class members have no other adequate remedy of law in that absent injunctive relief from the Court Defendants are likely to not fully redress the issues raised by their illegal and unfair business practices. Defendants have not announced any specific changes to their data security infrastructure, processes or procedures to fix the vulnerabilities in the electronic information security systems and/or security practices that permitted the Conti ransomware attack and the Data Breach to occur and go undetected, and thereby prevent further attacks, nor did they provide complete and prompt notice of the circumstances surrounding this breach as required by law.

129. Pursuant to Business & Professions Code section 17203, Plaintiff seeks an order of this Court both for himself, members of the Class and for the benefit of the public for injunctive relief in the form of requiring Defendants to correct their illegal conduct, to prevent Defendants from repeating the illegal and wrongful practices as alleged above and protect and preserve confidentiality of Personal Information and Medical Information in Defendants' possession that has been accessed, downloaded, exfiltrated, stolen, and viewed by at least one unauthorized third party because of Defendants' illegal and wrongful practices set forth above.

130. This action, if successful, will enforce an important right affecting the public interest and would confer a significant benefit, whether pecuniary or non-pecuniary, for a large class of persons and/or the general public. Private enforcement is necessary and places a disproportionate financial burden on Plaintiff in relation to Plaintiff's stake in the matter. Because this case is brought for the purposes of enforcing important rights affecting the public interest, Plaintiff also seeks the recovery of attorneys' fees and costs in prosecuting this action against Defendants under Code of Civil Procedure section 1021.5 and other applicable law.

FIFTH CAUSE OF ACTION

Declaratory Relief

131. Plaintiff incorporates the foregoing allegations by reference as if fully set forth herein.

132. A present and actual controversy exists between the parties. Defendants have failed to acknowledge the wrongful nature of their actions, have not sent affected patients comprehensive data breach notices regarding the Conti ransomware attack and Data Breach at issue herein, nor publicly issued comprehensive corrective notices. Based on their inadequate disclosures to date, there is also no reason to believe that Defendants have taken adequate measures to correct or enact adequate privacy policies and revised their IT and computer systems to protect and preserve Plaintiff's and the Class members' Personal Information and Medical Information in Defendants' possession.

133. Now that Defendants' insufficient information security is known to hackers, the Personal Information and Medical Information in Defendants' possession is even more vulnerable to cyberattack.

134. Plaintiff and the Class members have no other adequate remedy of law in that absent declaratory relief from the Court, Defendants are likely to not fully remedy the underlying wrong.

135. As described above, Defendants' actions have caused harm to Plaintiff and Class members. Further, Plaintiff and the Class members are at risk of additional or further harm due to the exposure of their Medical Information and Personal Information and Defendants' failure to fully address the security failings that lead to such exposure and provide notice thereof.

136. Plaintiff and the Class members seek an order of this Court for declaratory, equitable and/or injunctive relief in the form of an order finding Defendants have failed and continue to fail to adequately protect Plaintiff's and the Class members' Personal Information and Medical Information

from release to unknown and unauthorized third parties, requiring Defendants to correct or enact adequate privacy policies and security measures to protect and preserve Plaintiff's and the Class members' Personal Information and Medical Information in their possession, and requiring Defendants to publicly issue comprehensive corrective notices to Plaintiff, Class members and the public.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, both individually and on behalf of the Class and for the benefit of the public as applicable, prays for orders and judgment in favor of Plaintiff and against Defendants as follows, as applicable to the above Causes of Action:

A. Finding that this action satisfies the prerequisites for maintenance as a class action and certifying the Class defined herein;

B. Designating Plaintiff as representative of the Class and his counsel as Class counsel;

C. Declaring Defendants' conduct in violation of the laws set forth above, including California Civil Code sections 56.10(a), 56.10(e), 56.20, 56.101, 1798.150(a), 1798.82, Business and Professions Code § 17200 *et seq.*, and Article I, § 1 of the California Constitution.

D. An order:

1. prohibiting Defendants from engaging in the wrongful and unlawful acts described herein;

2. prohibiting Defendants from refusing to send all affected persons updated and comprehensive data breach notices regarding the ransomware attack and data theft at issue herein in the form and timing required by law, and publicly issue comprehensive corrective notices to Plaintiff, Class members and the public;

3. prohibiting Defendants from failing to protect, including through encryption, all data collected through the course of their business operations in accordance with all applicable regulations, industry standards, and federal and state laws;

4. prohibiting Defendants from refusing to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the Personal Information and Medical Information of Plaintiff and the Class

members;

5. prohibiting Defendants from refusing to engage independent third-party security auditors/penetration testers as well as internal security personnel to run automated security monitoring, database scanning and security checks and conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors;

6. prohibiting Defendants from refusing to audit, test, and train security personnel regarding any new or modified procedures;

7. requiring Defendants to segment data by, among other things, creating firewalls and access controls so that if one area of Defendants' network is compromised, hackers cannot gain access to other portions of Defendants' systems;

8. prohibiting Defendants from refusing to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class members and infiltration of Defendants' computer system by phishing processes by using such steps such as multi-factor authentication;

9. prohibiting Defendants from refusing to routinely and continually conduct internal training and education, and inform internal security personnel how to immediately identify and contain a ransomware attack or data breach when it occurs and what to do in response to a breach; and,

10. prohibiting Defendants from refusing to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendants' information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

E. Awarding Plaintiff and the Class Members all actual, compensatory, statutory, punitive and other damages, restitution and/or restitutionary disgorgement to which they are entitled under the causes of action set forth above;

F. Awarding Plaintiff's counsel reasonable attorneys' fees and non-taxable expenses and costs;

G. Awarding pre- and post-judgment interest at the maximum rate permitted by applicable law; and,

H. Granting such further relief as the Court deems just.

JURY DEMANDED

Plaintiff demands a trial by jury on all issues so triable.

Dated: June 2, 2022

Respectfully submitted,

WHATLEY KALLAS, LLP
Alan M. Mansfield, SBN: 125998
16870 W. Bernardo Drive
Suite 400
San Diego, CA 92127
Phone: (619) 308-5034
Fax: (888) 341-5048
Email: amansfield@whatleykallas.com

WHATLEY KALLAS, LLP
Joe R. Whatley, Jr. (*Pro Hac Vice application to be filed*)
jwhatley@whatleykallas.com
Edith M. Kallas (*Pro Hac Vice application to be filed*)
ekallas@whatleykallas.com
Patrick J. Sheehan (*Pro Hac Vice application to be filed*)
psheehan@whatleykallas.com
152 W. 57th Street, 41st Floor
New York, NY 10019
Tel: (212) 447-7060
Fax: (800) 922-4851

APRIL M. STRAUSS, A PC
April M. Strauss, SBN: 163327
2500 Hospital Drive, Bldg 3
Mountain View, CA 94040
Phone: (650) 281-7081
Email: astrauss@sfaclp.com

DOYLE APC
William J. Doyle, SBN: 188069
550 West B Street
4th Floor
San Diego, CA 92101
Phone: (619) 736-0000
Fax: (619) 736-1111
Email: bill@doyleapc.com

Attorneys for Plaintiff